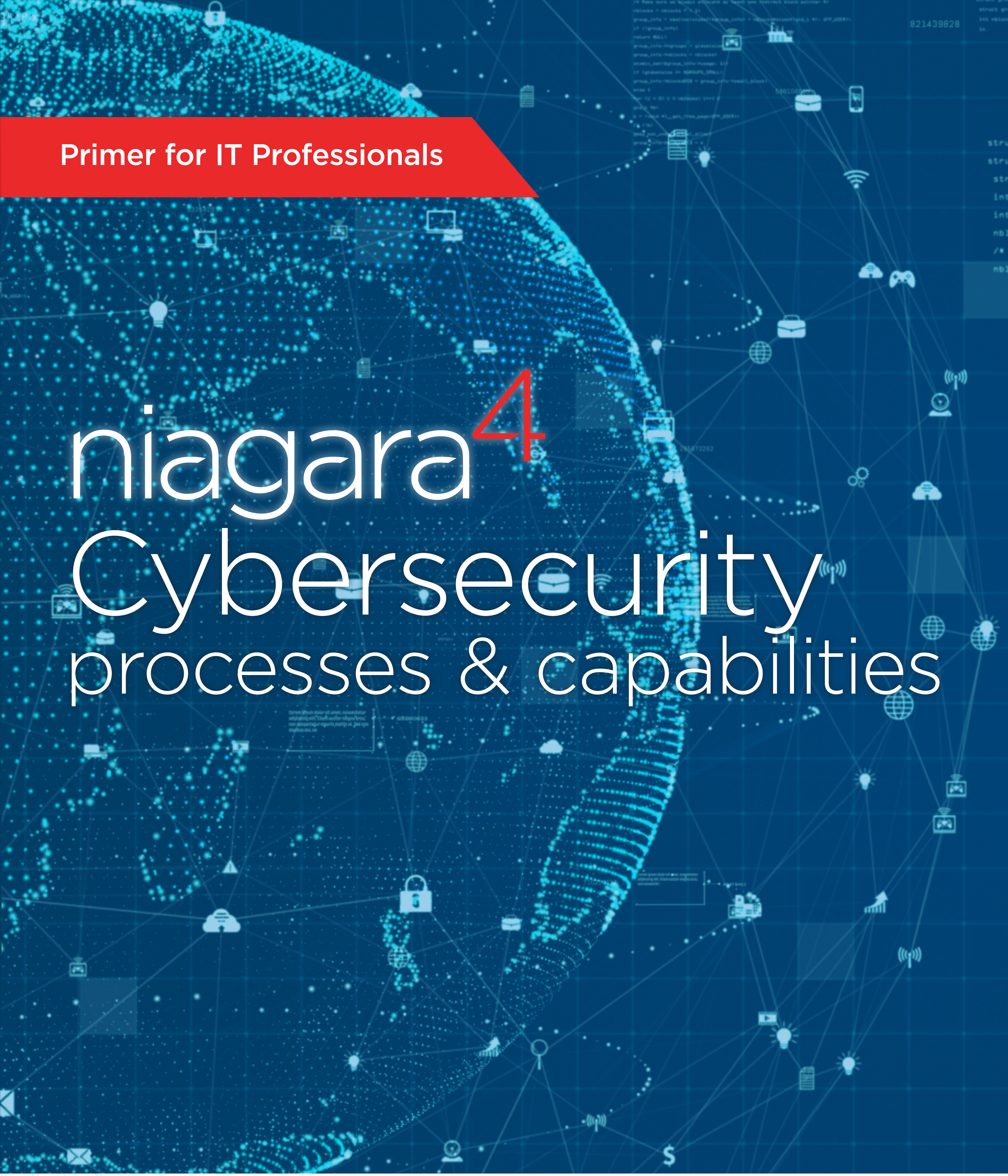


Primer for IT Professionals

niagara4 Cybersecurity processes & capabilities

TRIDIUM

TRIDIUM CYBER DEFENSE

First principle: “Secure by Default”

With almost one-quarter century of market growth and over 1 million instances deployed around the world, Niagara Framework® has achieved the status of ‘defacto industry standard’ for connecting and controlling diverse equipment and devices in buildings and beyond. With a vast user base comes great cyber defense responsibility. Here are the four steps we take in the design of our software and hardware to deliver products that are *secure by default*.

1 MAKE SECURITY EASIER

Tridium products are designed to default to the most secure configurations. Administrators are prompted through a secure set-up that requires strong, custom passwords. New user set-up only happens via a strong authentication mechanism. To make it easier for Niagara customers to practice good cyber hygiene, Niagara 4 now offers the Security Dashboard which displays security KPIs across a Niagara network at-a-glance so that corrective measures can happen proactively.

2 ENCRYPT DATA/VALIDATE CODE

Regardless of configuration, Tridium products are designed to protect data and equipment. Our JACE® 8000 Secure Boot process validates that only trusted software runs at boot-time. All modules of code must be digitally signed and this is validated at run-time. All transmissions are encrypted by default, and data-at-rest is also encrypted.

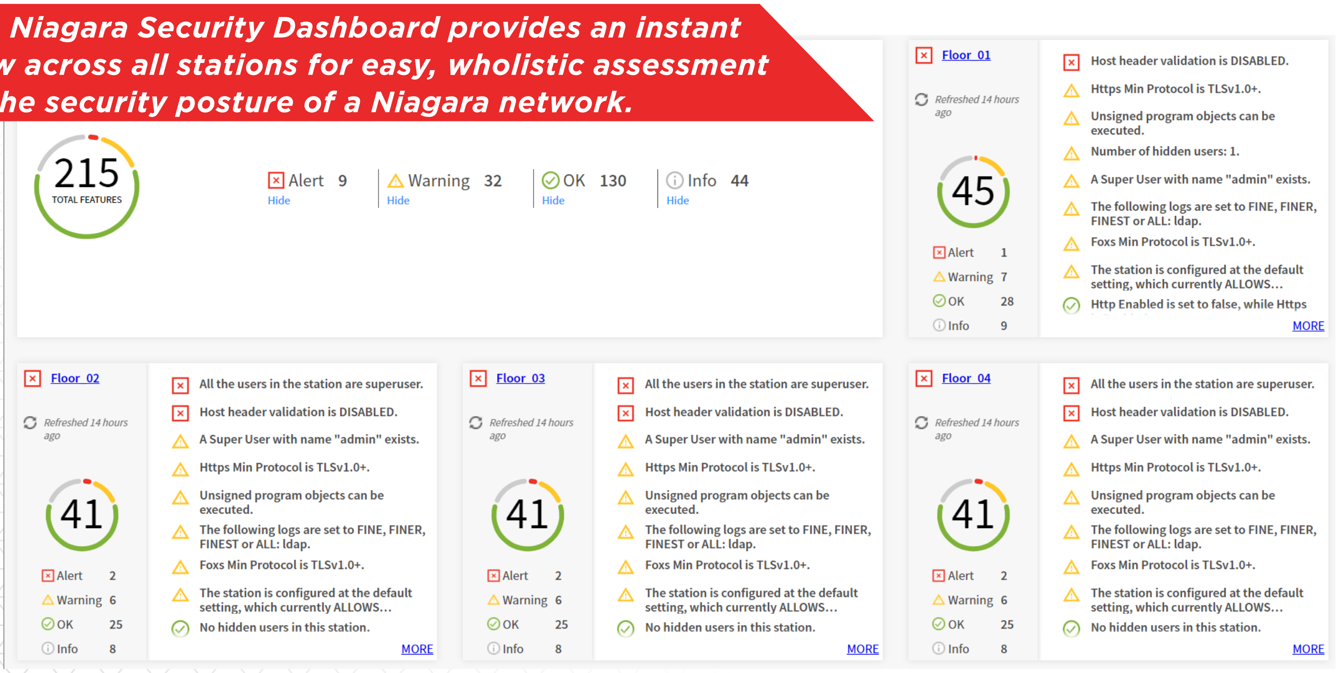
3 CONDUCT SECURE PRODUCT DEVELOPMENT PROCESSES

Tridium product development processes adhere to on-going review, audit, and risk management cycles as defined by security standards, particularly ISA 62443-3-3 which outlines processes appropriate for control and automation products used in critical infrastructure.

4 MODEL & PROMOTE BEST PRACTICES

Tridium is engaged with the IT industry and government entities defining enterprise security best practices, and we continuously build those practices into our configuration options. We also publish articles, documentation, and video tutorials to provide detailed cyber-security guidance to users.

The Niagara Security Dashboard provides an instant view across all stations for easy, wholistic assessment of the security posture of a Niagara network.



215 TOTAL FEATURES

☒ Alert 9 Hide | ⚠ Warning 32 Hide | ✓ OK 130 Hide | ⓘ Info 44 Hide

☒ Floor_01

Refreshed 14 hours ago

45

☒ Alert	1
⚠ Warning	7
✓ OK	28
ⓘ Info	9

☒ Host header validation is DISABLED.
⚠ Https Min Protocol is TLSv1.0+.
⚠ Unsigned program objects can be executed.
⚠ Number of hidden users: 1.
⚠ A Super User with name "admin" exists.
⚠ The following logs are set to FINE, FINER, FINEST or ALL: ldap.
⚠ Foxs Min Protocol is TLSv1.0+.
⚠ The station is configured at the default setting, which currently ALLOWS...
✓ Http Enabled is set to false, while Https

MORE

☒ Floor_02

Refreshed 14 hours ago

41

☒ Alert	2
⚠ Warning	6
✓ OK	25
ⓘ Info	8

☒ All the users in the station are superuser.
☒ Host header validation is DISABLED.
⚠ A Super User with name "admin" exists.
⚠ Https Min Protocol is TLSv1.0+.
⚠ Unsigned program objects can be executed.
⚠ The following logs are set to FINE, FINER, FINEST or ALL: ldap.
⚠ Foxs Min Protocol is TLSv1.0+.
⚠ The station is configured at the default setting, which currently ALLOWS...
✓ No hidden users in this station.

MORE

☒ Floor_03

Refreshed 14 hours ago

41

☒ Alert	2
⚠ Warning	6
✓ OK	25
ⓘ Info	8

☒ All the users in the station are superuser.
☒ Host header validation is DISABLED.
⚠ A Super User with name "admin" exists.
⚠ Https Min Protocol is TLSv1.0+.
⚠ Unsigned program objects can be executed.
⚠ The following logs are set to FINE, FINER, FINEST or ALL: ldap.
⚠ Foxs Min Protocol is TLSv1.0+.
⚠ The station is configured at the default setting, which currently ALLOWS...
✓ No hidden users in this station.

MORE

☒ Floor_04

Refreshed 14 hours ago

41

☒ Alert	2
⚠ Warning	6
✓ OK	25
ⓘ Info	8

☒ All the users in the station are superuser.
☒ Host header validation is DISABLED.
⚠ A Super User with name "admin" exists.
⚠ Https Min Protocol is TLSv1.0+.
⚠ Unsigned program objects can be executed.
⚠ The following logs are set to FINE, FINER, FINEST or ALL: ldap.
⚠ Foxs Min Protocol is TLSv1.0+.
⚠ The station is configured at the default setting, which currently ALLOWS...
✓ No hidden users in this station.

MORE

SECURITY PRACTICES

Tridium operates its product development organization to security standards set by ISA 62443-3-3, Security Level 4 for Critical Infrastructure. This aims for a level of protection calibrated to thwart intentional security violations up to and including those using sophisticated means and extended resources, perpetrated by people with IACS-specific skills and high motivation. Here are some of the practices put in place to achieve this level of defense.

Category	Practice
Internal Reviews	• Security Design Reviews/Security Code Reviews • Security Threat Modeling • Automated Security Tests for ISA 62443-3-3 Security Requirements • Reviews for vulnerabilities in third party libraries • Static Code Analysis and Binary Code Analysis • Risks managed in Risk Register according to CVSS Score
Security Testing	• Routine and periodic detailed and robust security testing by internal and external organizations on new and existing releases • Testing partners include deep penetration testing by internal testing teams, external commercial security partners, and government customers • Procedures include penetration testing, abuse case testing, white box/black box testing, security design reviews, and security code reviews
Internal Audits	• 5 phase auditing process, whereby all security artifacts from above are reviewed. CTO must sign-off before Tridium CCB meets to vote on each phase
Risk Management	• All known security vulnerabilities have visibility at the highest levels of enterprise governance • 30-day, 60-day, 90-day, 120-day requirements are set based on CVSS Score • Deadlines on mitigating all found threats are enforced
Incident Response	• Robust process for investigating vulnerabilities, mitigating threats, and communication response • Product Security Incident Response Team (PSIRT) works to respond to externally reported vulnerabilities, working with all parties involved to mitigate and resolve issues. PSIRT issues may be reported to security@tridium.com or go to https://www.honeywell.com/us/en/product-security#vulnerability-reporting
Support	• Potential vulnerabilities are addressed with code patches in a timely and efficient manner • Security update builds are added to the release schedule • Niagara user community is advised to apply patches and security updates via timely and distinct communications

Standards & Protocols

AUTHENTICATION

- SCRAM-SHA (256/512 bit) DIGEST–default
- JACE-8000: WPA-PSK128, WPA2PSK256
- Google 2-factor Auth, Client Cert Auth (Kiosk Mode)
- As of Niagara 4.9, SAML Identity Provider (IDP) included for use with SAML-based Single-Sign-On
- LDAP & SAML 2 SSO authentication

IDENTITY INFRASTRUCTURE

- PKI, LDAP, Kerberos authentication
- Integration with SAML 2 SSO IDPs (since Niagara 4.4)

ENCRYPTED COMMUNICATIONS

- TLS 1.2, 1.1, 1.0 (FOXS / HTTPS) , issued with RSA 2048-bit certificate, SHA256withRSA
- By default, only perfect-forward secrecy ciphers are used
- TLS 1.3

ENCRYPTION AT REST

- AES 256-CBC Symmetric Key Encryption (As of Niagara 4.9: AES GCM)
- PBKDF2-HMAC-SHA256

DIGITAL SIGNATURES

- SHA256withRSA (2048-bit RSA asymmetric key)

COMPLIANCE

- 4.6 and above: FIPS 140-2 Compliance using FIPS 140-2 cryptographic module
- For US Federal Government, DoD Risk Management Framework (RMF), artifacts for Niagara 4 available in SAFE

USER AUTHORIZATION

- RBAC (Role-Based Access Control)

USER ACCOUNT MANAGEMENT

- OWASP recommendations

GENERAL SECURITY REQUIREMENTS

- All security requirements for Niagara derived from ISA 62443 Security Level 4

We provide strong security capabilities – but it is important for our partners and customers to configure and manage Niagara according to robust cyber defense and security best practices!

TRIDIUM

Tridium advances an *open* approach to the challenges of systems integration, data normalization and interoperability. Our Niagara Framework® software products and JACE® devices allow diverse monitoring, control and automation systems to communicate and collaborate in buildings, data centers, manufacturing systems, smart cities and beyond. We create smarter, safer and more efficient enterprises and communities—bringing intelligence and connectivity to the network edge and back. You can buy Tridium products through many partners and distribution channels, including equipment manufacturers (OEMs), industrial product distributors, independent systems integrators, independent software vendors (ISVs) and other technology companies. Our open distribution business model and open protocol support allow a vendor-neutral application compatible with devices and systems throughout the world.

Subscribe at www.tridium.com to receive our product information, including Technical Bulletins.

TRIDIUM

tridium.com

Locations and customer support, worldwide

Headquarters
North America
1 804 747 4771

Support
North America & Latin America
1 877 305 1745

Europe, Middle East & Africa
44 1403 740290

Asia Pacific
86 400 818 6088

Information and/or specifications published here are current as of the date of publication of this document. Tridium, Inc. reserves the right to change or modify specifications without prior notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia. Products or features contained herein may be covered by one or more U.S. or foreign patents. This document may be copied only as expressly authorized by Tridium in writing. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form.